ETSETB
Curso 2009-10 Otoño
EXAMEN DE TRANSMISIÓN DE DATOS
7 de enero de 2010

Publicación de notas provisionales: 12/01/2010
Fecha límite para las alegaciones: 15/01/2010
Publicación de notas definitivas: 20/01/2010

NOTAS IMPORTANTES:

- Toda hoja de respuestas que no esté completamente identificada será anulada. La numeración en la hoja de respuestas es la de la *izquierda* (*correlativas*)
- No se responderá a ninguna pregunta sobre el enunciado. El alumno responderá según su criterio pudiendo realizar las alegaciones que considere oportunas por escrito en la secretaría de la ETSETB a partir de la publicación de las calificaciones provisionales y hasta el plazo arriba indicado. En ellas debe consignarse OBLIGATORIAMENTE el DNI y el código de la prueba. Queda expresamente prohibido el uso de cualquier dispositivo de comunicación.

CÓDIGO DE LA PRUEBA: 230 11510 00 1

1. Indique cuál de las siguientes afirmaciones es FALSA
   a) Siendo $135529 = 433 * 313$, se verifica que $42059^{134783} \bmod 135529 = 2710$
   b) El número de elementos que tienen inversa respecto a la operación producto en Z_{77} es 60
   c) $27^{30} \bmod 31 = 1$
   d) Alguna de las anteriores es falsa
2. Sea un código de Hamming caracterizado por $g(D) = (D+1)(D^3+D+1)$. Puede afirmarse que:
   a) La eficiencia del código es del 73.3 %.
   b) La ráfaga de error $e(D) = D^{11} + D^4$ es detectable
   c) El código tiene una capacidad correctora de 3 borrones
   d) Ninguna de las anteriores
3. Sea un cifrador en flujo compuesto por dos LFSR cuyas salidas se unen en una puerta XOR para entregar la secuencia cifrante S. Los polinomios de conexiones asociados son: $C_1(D) = D^5 + D^2 + 1$ (primitivo); $C_2(D) = D5 + D4 + D3 + D2 + D + 1$. El estado inicial en cada LFSR es $S(D) = 1$. El periodo de la secuencia S vale:
   a) 186
   b) 6
   c) 31
   d) Ninguna de las anteriores
4. Un atacante sabe que dos usuarios castellanos utilizan indistintamente un cifrado de César o un cifrado de transposición consistente en una matriz de un número dado de columnas. El atacante ha capturado dos criptogramas relativos a un mismo mensaje: C1 = {M E D O A S E X Ñ O E X A C N X N H E X A O R X} y C2 = {R G T G S G K Y U I M U J K K S K X U}. El atacante deduce que:
   Nota.- En la figura 2 se muestra la frecuencia de letras en castellano
   a) El mensaje es cierto.
   b) C1 y C2 son cifrados de César.
   c) C1 es un cifrado de César y C2 es un cifrado de transposición.
   d) Ninguna de las anteriores.
5. Sea el código polinómico con polinomio generador $g(D) = D^5 + D^4 + D^2 + 1$ de longitud n=17. ¿Qué afirmación es correcta?
   a) No detecta un número impar de errores
   b) El error $e(D) = D^9 + D^6 + D^4 + D^3$ se detecta con probabilidad 0.9375
   c) Detecta todos los errores dobles
   d) Ninguna de las anteriores
6. La fuente de un sistema de transmisión de datos tiene un alfabeto de 10 símbolos {0, 1, ..., 9} Cuando el elemento enviado pertenece al conjunto {1, 2, ..., 9} se recibe correctamente, mientras que si el elemento enviado es un 0 se recibe uno del conjunto {1, 2, ..., 9} con probabilidad directamente proporcional al número (por ejemplo, si se envía un 0, la probabilidad de recibir un 5 es 5 veces la probabilidad de recibir un 1).Calcule la capacidad del canal discreto
   a) 3.35 bits/simb.
   b) 3.28 bits/simb.
   c) 3.17 bits/simb.
   d) Ninguna de las anteriores
7. Sabiendo que la información mutua entre dos variables aleatorias A y B $I(A;B) > 0$, es FALSO que
   a) $H(A,B) < H(A) + H(B)$
   b) $H(A/B) > H(A) - H(B)$
   c) $H(B/A) < H(B)$
   d) Alguna de las anteriores es falsa
8. La probabilidad p de no detección de errores en un código Hamming de redundancia 3, para una BER (*Bit Error Rate*) de 10^{-3}, es:
   a) $10^{-9} < p \leq 2 * 10^{-8}$
   b) $2 * 10^{-8} < p \leq 5 * 10^{-8}$
   c) $p \leq 10^{-9}$
   d) $5 * 10^{-8} < p$
9. Una fuente binaria tiene las siguientes propiedades: P(B)=1/3, P(B/B)=0.2. Calcule la eficiencia de una codificación de Huffman extendido de orden 1 (agrupaciones de 2 símbolos)
   a) $0{,}77 \leq E < 0{,}85$
   b) $0{,}85 \leq E < 0{,}93$
   c) $E < 0{,}77$
   d) $E \geq 0{,}93$
10. Sean F1 = {1, 2, 3} y F2 = {2, 4, 6, 8} dos fuentes equiprobables independientes. Sea una fuente (F) cuya salida es el mínimo común múltiplo de la salida de las fuentes anteriores F = mcm(F1, F2). La entropía (en bits) de F condicionada al valor 6 de F2, $H(F|F2 = 6)$ vale:
    a) 0.9
    b) 1
    c) 0
    d) Ninguna de las anteriores

11. Sea una fuente discreta sin memoria que emite cuatro símbolos con probabilidades P(A)=P(B)=1/3; P(C)=2/9; P(D)=1/9. La eficiencia de una codificación de Huffman ternaria vale aproximadamente:

    a) 0.7823

    b) 0.8948

    c) 1

    d) Ninguna de las anteriores

12. Un código ISBN-10 es un código detector de errores no binario (trabaja sobre Z_{11}), e introduce un digito de redundancia a los 9 de información. Suponga que un ISBN introducido correctamente se transmite a través de un canal sin memoria donde la probabilidad de recibir incorrectamente un dígito es $p = 10^{-4}$ y posteriormente se almacena en el receptor. Suponiendo que todo ISBN-10 erróneo detectado se retransmite correctamente, ¿Cuánto vale aproximadamente la probabilidad de que un ISBN-10 incorrecto se almacene en el receptor?

    a) $4{,}1 * 10^{-8}$

    b) 10^{-8}

    c) $4{,}5 * 10^{-7}$

    d) Ninguna de las anteriores

13. Se conoce la entropía conjunta entre dos variables aleatorias, expresada en la tabla. ¿Qué afirmación es correcta?

X,Y	Y_1	Y_2	Y_3
X_1	0	1/6	1/3
X_2	1/3	1/6	0

    a) $0{,}4 \leq H(Y|X) \leq 0{,}5$ bits/simb.

    b) $0{,}3 \leq H(X|Y) \leq 0{,}4$ bits/simb.

    c) $0{,}8 \leq I(X;Y) \leq 0{,}9$ bits/simb.

    d) Ninguna de las anteriores

14. En un sistema RSA hay dos usuarios A y B y un atacante. Todos los usuarios utilizan el mismo módulo $N = 4559$. La clave pública de A es $e_A = 7$ y la de B es $e_B = 17$. A y B se intercambian los dos un mismo mensaje M cifrado y el atacante intercepta estos criptogramas: $C_{A->B} = 3227$ y $C_{B->A} = 1872$. El atacante intenta descubrir el mensaje M.

    Nota1.- 3227*4227 = 1 mod 4559, 1872*1639=1 mod 4559

    Nota2.- Listado de los números primos hasta 100: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 y 97.

    a) $M = 60$

    b) $M = 20$

    c) No puede hallarlo

    d) Ninguna de las anteriores

15. La matriz generadora de un código lineal binario C(6, 3) es:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

    ¿Qué afirmación es correcta?

    a) Si se recibe Z=100110, los mensajes 010, 100 y 110 son igual de verosímiles

    b) Si se recibe Z=10*1*0, el mensaje estimado es 100

    c) Si se recibe Z=100100, el mensaje estimado es 101

    d) e) Ninguna de las anteriores

16. ¿Cuál de las siguientes puede ser una matriz de comprobación de un código sistemático binario con capacidad de corrección 2?

    a) $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

    b) $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

    c) $H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$

    d) Ninguna de las anteriores

17. Un LFSR de 4 celdas tiene periodo 13 cuando el estado inicial es $S(D) = D^3 + D^2 + D + 1$. Indique la respuesta correcta.

    a) El polinomio de realimentación puede ser irreducible

    b) El cifrador trabaja en modo autosincronizante

    c) El polinomio de realimentación es primitivo

    d) Ninguna de los anteriores

18. Sabiendo que $N = 9797$ tiene divisores cercanos a su media geométrica, calcule $X = 7^{96005} \bmod 9797$

    a) 1816

    b) 7010

    c) 3243

    d) Ninguna de las anteriores

19. Calcule la capacidad de canal para un canal discreto binario simétrico como el de la *figura 1*, que introduce un borrón (símbolo *) en el destino

    a) 0,1 bits/simb $< C \leq$ 0,2 bits/simb.

    b) 0,2 bits/simb $< C \leq$ 0,5 bits/simb.

    c) 0 bits/simb $\leq C \leq$ 0,1 bits/simb.

    d) 0,5 bits/simb $< C$

20. En un paquete de 9 bits de datos útiles, se añade una redundancia de acuerdo a código polinómico, cuyo polinomio generador es $g(D) = (D^4 + D + 1)(D + 1)$. Indicar cuál de las siguientes respuestas es correcta

    a) Si el número de errores es impar, la probabilidad de detección es 31/32

    b) No todas las situaciones con 2 errores son detectables

    c) Si el número de errores es 2, el código siempre los puede corregir

    d) Ninguna de las anteriores

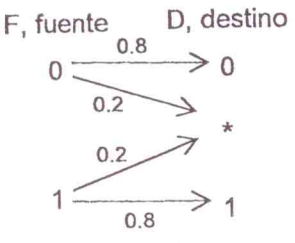
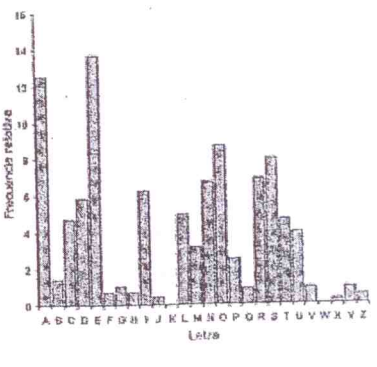


Figura 1



ETSETB
Curso 2009-10 Otoño
EXAMEN DE TRANSMISIÓN DE DATOS
7 de enero de 2010

PUBLICACIÓN DE NOTAS PROVISIONALES: 12/01/2010 A ~~LAS X:00 HORAS~~
FECHA LÍMITE PARA LAS ALEGACIONES: 15/01/2010 a ~~las 14:00 horas~~
PUBLICACIÓN DE NOTAS DEFINITIVAS: 20/01/2010

NOTAS IMPORTANTES:

- Toda hoja de respuestas que no esté completamente identificada será anulada.
- La numeración en la hoja de respuestas es la de la *izquierda* (*correlativas*)
- No se responderá a ninguna pregunta sobre el enunciado. El alumno responderá según su criterio pudiendo realizar las alegaciones que considere oportunas por escrito en la secretaría de la ETSETB a partir de la publicación de las calificaciones provisionales y hasta el plazo arriba indicado. En ellas debe consignarse OBLIGATORIAMENTE el DNI y el código de la prueba.
- QUEDA EXPRESAMENTE PROHIBIDO EL USO DE CUALQUIER DISPOSITIVO DE COMUNICACIÓN. EL INCUMPLIMIENTO DE ESTA NORMA SUPONDRÁ LA EXPULSIÓN DEL EXAMEN.

CÓDIGO DE LA PRUEBA: 230 11510 00 0

1. Sea el código polinómico con polinomio generador $g(D) = D^5 + D^4 + D^2 + 1$ de longitud n=17. ¿Qué afirmación es correcta?

   a) Detecta todos los errores dobles
   b) No detecta un número impar de errores
   c) El error $e(D) = D^9 + D^6 + D^4 + D^3$ se detecta con probabilidad 0.9375
   (*d*) Ninguna de las anteriores

$D^5 + D^4 + D^2 + 1 \;\; \lfloor D+1$
$D^5 + D^4 \qquad\qquad D^4 + D + 1$
$D^2 + 1$
$D^2 + D$
$D + 1$
$D + 1$
0

$g(D) = D^5 + D^4 + D^2 + 1 = (D+1)\cdot(D^4 + D + 1)$

b) $g(D)$ detecta los errores impares: $e(D=1) = 1 \rightarrow (D+1)$ no es factor de $e(D)$ con número impar términos.

primo, $m = 4$
$L = 2^m - 1 = 15$
- divide a $D^4 + 1$.
- no divide a $D^j + 1$, $j < L$.

a) $e(D) = D^j + D^i = D^i \cdot (D^{j-i} + 1)$

$g(D)$ no dividirá a $e(D)$ si $j - i < L = 2^m - 1$

$\vec{e}_n = b_{n-1} \dots b_1 b_0 \Rightarrow e(D) = b_{n-1} D^{n-1} + \dots + b_1 D + b_0$
$b_i \in \{0, 1\}$

Los dos errores estarán separados como mucho $n-1$.
Si $n-1 < 2^m - 1$, se detectan todos los errores dobles.

$\rightarrow n < 2^m \rightarrow$ ¿$17 < 2^4 = 16$? NO. Por tanto, no todos los errores dobles se detectan. (cont→)

2. En un sistema RSA hay dos usuarios A y B y un atacante. Todos los usuarios utilizan el mismo módulo $N = 4559$. La clave pública de A es $e_A = 7$ y la de B es $e_B = 17$. A y B se intercambian los dos un mismo mensaje M cifrado y el atacante intercepta estos criptogramas: $C_{A->B} = 3227$ y $C_{B->A} = 1872$. El atacante intenta descubrir el mensaje M.

Nota1.- 3227*4227 = 1 mod 4559, 1872*1639=1 mod 4559

Nota2.- Listado de los números primos hasta 100: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 y 97.

a) No puede hallarlo

b) $M = 60$

c) $M = 20$

d) Ninguna de las anteriores

Ataque por módulo común: $\text{mcd}(e_A, e_B) = 1$. $\exists\ r, s \in \mathbb{Z}_n \mid r \cdot e_A + s \cdot e_B = 1$

$r \cdot 7 + s \cdot 17 = 1$

17 | 7	7 | 3	3 | 1
3 | 2	(1) | 2	0 | 3
	= mcd(17,7)	

$17 = 7 \cdot 2 + 3$

$7 = 3 \cdot 2 + 1$

Algoritmo Extendido de Euclides,

$3 = 17 - 7 \cdot 2 \rightarrow 7 = (17 - 7 \cdot 2) \cdot 2 + 1 = 17 \cdot 2 - 7 \cdot 4 + 1$

$7(1+4) - 17 \cdot 2 = 1 \rightarrow 7 \cdot 5 - 17 \cdot 2 = 1 \rightarrow r = 5,\ s = -2$

$C_{AB} = M^{e_B} \bmod N$

$C_{BA} = M^{e_A} \bmod N$

$C_{AB}^{s} \cdot C_{BA}^{r} = M^{e_B \cdot s} \cdot M^{r \cdot e_A} = M^{r \cdot e_A + s \cdot e_B} = M \bmod N$

$M = 3227^{-2} \cdot 1872^{5} \bmod N = (3227^{-1})^2 \bmod N \cdot 1875^{5} \bmod N$

$3227^{-1} \bmod N = 4227$

$M = 4227^{2} \bmod 4559 \cdot 1875^{5} \bmod 4559 = 808 \cdot 790 \bmod 4559 = 60$

1) cont.

c) $e(D) = D^9 + D^6 + D^4 + D^3 \rightarrow e(D) \bmod g(D) \neq 0 \rightarrow$ Se detecta con prob. 100%

$D^9 + D^6 + D^4 + D^3 \ \big|\ D^5 + D^4 + D^2 + 1$

$D^9 + D^8 + D^6 + D^4 \quad\quad D^4 + D^3 + D^2 + D$

$D^8 + D^3$

$D^8 + D^7 + D^5 + D^3$

$D^7 + D^5$

$D^7 + D^6 + D^4 + D^2$

$D^6 + D^5 + D^4 + D^2$

$D^6 + D^5 + D^3 + D$

$D^4 + D^3 + D^2 + D \neq 0$

ERROR

$\vec{e}_n = 1\,0\,0\,1\,0\,1\,1\,0\,0\,0$ ($\ell = 7$)

$r = 5$ $\quad \ell$ = long. ráfaga

$\ell > r + 1$ — prob $= 1 - \frac{1}{2^{r-1}} =$

$= 1 - \frac{1}{2^4} = \frac{15}{16} = 93'75\%$

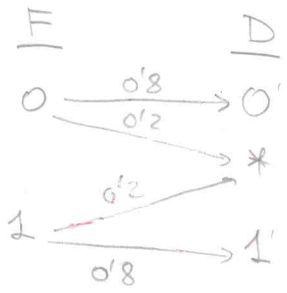
3. Calcule la capacidad de canal para un canal discreto binario simétrico como el de la *figura 1*, que introduce un borrón (símbolo *) en el destino

   a) 0 bits/simb $\leq C \leq$ 0,1 bits/simb.

   b) 0,1 bits/simb $< C \leq$ 0,2 bits/simb.

   c) 0,2 bits/simb $< C \leq$ 0,5 bits/simb.

   d) 0.5 bits/simb $< C$



$$p(D|F) = \begin{pmatrix} 0'8 & 0'2 & 0 \\ 0 & 0'2 & 0'8 \end{pmatrix}$$

$$H(D|F) = 0'8 \cdot \log_2 \frac{1}{0'8} + 0'2 \log_2 \frac{1}{0'2} = 0'7219 \ \frac{\text{bits}}{\text{símbolo}}$$

$$C = \max_F \{H(D) - H(D|F)\} = \max_F H(D) - 0'7219$$

$p(0') = 0'8 \cdot p(0)$

$p(*) = 0'2 \cdot p(0) + 0'2\, p(1) = 0'2 \cdot (p(0) + p(1)) = 0'2$

$p(1') = 0'8 \cdot p(1)$

¿ $\exists\ F \mid p(0') = p(*) = p(1') = \frac{1}{3}$? → No, por lo que $H(D) < \log_2 3$.

$$H(D) = 0'8 \cdot p(0) \cdot \log_2 \frac{1}{0'8 \cdot p(0)} + 0'2 \cdot \log_2 \frac{1}{0'2} + 0'8 \cdot p(1) \cdot \log_2 \frac{1}{0'8 \cdot p(1)} =$$

$$= 0'8 \cdot p(0) \left(\log_2 \frac{1}{0'8} + \log_2 \frac{1}{p(0)} \right) + 0'2 \log_2 \frac{1}{0'2} + 0'8 \cdot p(1) \cdot \left(\log_2 \frac{1}{0'8} + \log_2 \frac{1}{p(1)} \right) =$$

$$= 0'8 \cdot \log_2 \frac{1}{0'8} \cdot \underbrace{(p(0) + p(1))}_{1} + 0'8 \left(p(0) \cdot \log_2 \frac{1}{p(0)} + p(1) \cdot \log_2 \frac{1}{p(1)} \right) + 0'2 \log_2 \frac{1}{0'2}$$

$$= 0'7219 + 0'8 \cdot H(x)$$

$$C = \max_F \left\{ 0'7219 + 0'8\, H(x) - 0'7219 \right\} = 0'8 \max_{\underbrace{p(x_i)}_{\log_2 2 = 1 \text{ bit/símbolo}}} H(x) = 0'8 \ \text{bits/símbolo}$$

$p(0) = p(1) = \frac{1}{2}$

4. Un atacante sabe que dos usuarios castellanos utilizan indistintamente un cifrado de César o un cifrado de transposición consistente en una matriz de un número dado de columnas. El atacante ha capturado dos criptogramas relativos a un mismo mensaje: C1 = {M E D O A S E X Ñ O E X A C N X N H E X A O R X} y C2 = {R G T G S G K Y U I M U J K K S K X U}. El atacante deduce que:

Nota.- En la figura 2 se muestra la frecuencia de letras en castellano

a) C1 es un cifrado de César y C2 es un cifrado de transposición.

b) El mensaje es cierto.

c) C1 y C2 son cifrados de César

d) Ninguna de las anteriores.

C1 = MEDO A SE X ÑO E X A C N X N H E X A O R X → hay 24 letras

E = 16% = 4/24 A = 12'5% = 3/24 O = 8'3% = 2/24 = castellano = letras } trasposición

C2 = R G T G S G K Y U I M U J K K S K X U D D D D D → hay 24 letras

K = 16% G = 12'5% U = 8'3% = castellano ≠ letras } César

clave césar = 6

a b c d e f g h i j k l ll m n ñ o p q r s t u v w x y z
G H I J K L LL M N Ñ O P Q R S T U V W X Y Z A B C D E F

C2 → m a ñ a n a e s o c h o d e e n e r o x x x x x (relleno)

MAÑANA
ESOCHO
DEENER
OXXXXX

→ MEDOASEXÑOEXACNXNHEXAORX

probabilidad

5. Se conoce la ~~entropía~~ conjunta entre dos variables aleatorias, expresada en la tabla. ¿Qué afirmación es correcta?

X,Y	Y_1	Y_2	Y_3
X_1	0	1/6	1/3
X_2	1/3	1/6	0

a) $0.8 \leq I(X;Y) \leq 0{,}9$
b) $0.4 \leq H(Y|X) \leq 0{,}5$
c) $0.3 \leq H(X|Y) \leq 0{,}4$
d) Ninguna de las anteriores

$p(x_1) = 0 + \frac{1}{6} + \frac{1}{3} = \frac{1}{2}$
$p(x_2) = \frac{1}{3} + \frac{1}{6} + 0 = \frac{1}{2}$
$\Big\}$ $H(x) = 2 \cdot \frac{1}{2} \log_2 \frac{1}{1/2} = 1$ bit/símbolo

$p(y_1) = 0 + \frac{1}{3} = \frac{1}{3}$
$p(y_2) = \frac{1}{6} + \frac{1}{6} = \frac{1}{3}$
$p(y_3) = \frac{1}{3} + 0 = \frac{1}{3}$
$\Big\}$ $H(Y) = 3 \cdot \frac{1}{3} \log_2 \frac{1}{1/3} = \log_2 3 = 1'5849$ bits/símbolo

$H(x,y) = 2 \cdot \frac{1}{6} \log_2 6 + 2 \cdot \frac{1}{3} \log_2 3 = 1'9183$ bits/símbolo

$H(x,y) = H(x) + H(y|x) = H(y) + H(x|y)$

$H(y|x) = 1'9183 - 1 = 0'9183$ bits/símbolo $\rightarrow$ b) NO

$H(x|y) = 1'9183 - 1'5849 = 0'3333$ bits/símbolo $\rightarrow$ c) Sí

$I(x;y) \Big\{ = H(x) - H(x|y) = 1 - 0'3333 = 0'6666$ bits/símbolo $\rightarrow$ a) NO
$\quad\quad = H(y) - H(y|x) = 1'5849 - 0'9183 = 0'6666$ bits/símbolo

6. La matriz generadora de un código lineal binario C(6, 3) es:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

¿Qué afirmación es correcta?

a) Si se recibe Z=100100, el mensaje estimado es 101

b) Si se recibe Z=100110, los mensajes 010, 100 y 110 son igual de verosímiles

c) Si se recibe Z=10*1*0, el mensaje estimado es 100

d) e) Ninguna de las anteriores

$$G = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right) = G_{k\times n} = (I_k \mid P)$$

Código → (6, 3), n, k

000 000	$= Y_0$
001 111	$= Y_1$
010 110	$= Y_2$
011 001	$= Y_1 + Y_2$
100 011	$= Y_4$
101 100	$= Y_4 + Y_1$
110 101	$= Y_2 + Y_4$
111 010	$= Y_1 + Y_2 + Y_4$

$d_{min} = 3$, $e = 1$, $s = 2$, $\rho = 2$

b)

$d(Z, Y)$	$\hat{X}$
3	
3	
2	→ 010
6	
2	→ 100
2	→ 101
3	
3	

$$H_{r\times n} = (-P^T \mid I_r) = \left(\begin{array}{ccc|ccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

a) $\vec{S_r} = Z \cdot H^T = (100100) \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = 111 = 3^{\text{a}}$ fila $H^T \Rightarrow \vec{e} = 001000$

$\hat{Y} = Z + \vec{e} = 100100 + 001000 = \underbrace{101}_{\hat{X}}100$

c) $\vec{S_r} = Z \cdot H^T = (10a1b0) \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = (1+a \quad 1+a+b \quad 1+a) \equiv (0\ 0\ 0)$

2 borrones $\leq \rho = 2$

$a = 1$, $b = 0$ $\Rightarrow \hat{Y} = \underbrace{101}_{\hat{X}}100$

7. La probabilidad p de no detección de errores en un código Hamming de redundancia 3, para una BER (*Bit Error Rate*) de 10^{-3}, es:

a) $p \leq 10^{-9}$
b) $10^{-9} < p \leq 2 * 10^{-8}$
c) $2 * 10^{-8} < p \leq 5 * 10^{-8}$
d) $5 * 10^{-8} < p$

$2^r = \binom{n}{0} + \binom{n}{1} = 1 + n$ $\quad r=3 \rightarrow n = 2^3 - 1 = 7 \rightarrow k = 4$

$C(7,4) \rightarrow e=1, \delta=2$ errores detecta (hasta)

Prob. NO detección $= 1 - p(\#\text{errores} \leq \delta \text{ errores})$

$= p(\#\text{errores} > \delta)$

Prob. NO detección $= 1 - p(0\text{ error}) - p(1\text{ error}) - p(2\text{ error}) = 3'4895 \cdot 10^{-8}$

$p(0\text{ error}) = (1-p)^n = (1-10^{-3})^7 = 0'9930$

$p(1\text{ error}) = \binom{n}{1} p (1-p)^{n-1} = 7 \cdot 10^{-3} \cdot (1-10^{-3})^6 = 6'9581 \cdot 10^{-3}$

$p(2\text{ error}) = \binom{n}{2} p^2 (1-p)^{n-2} = \frac{7 \cdot 6}{2} \cdot 10^{-6} \cdot (1-10^{-3})^5 = 2'08952 \cdot 10^{-5}$

Prob. NO detección $= \sum_{i=\delta+1}^{n} \binom{n}{i} p^i (1-p)^{n-i} \simeq$

$\simeq \binom{n}{\delta+1} p^{\delta+1} (1-p)^{n-\delta-1} = \underbrace{\binom{7}{3}}_{35} (10^{-3})^3 (0.999)^4 \simeq$

$\simeq \binom{7}{3} \cdot 10^{-9} = 35 \cdot 10^{-9} =$

$= 3'5 \cdot 10^{-8}$

8 ¿Cuál de las siguientes puede ser una matriz de comprobación de un código sistemático binario con capacidad de corrección 2?

a) $H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$

b) $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

c) $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

d) Ninguna anteriores (~~ponemos todas las anteriores matrices (9,4)~~)

CORRECTA: D.
Si H es 5*9, el código es (9,4). Para que la capacidad de corrección fuese 2 sería necesario que
Número de síndromes (2^5) >= 1+9+9*8/2, y podemos ver que eso no se cumple

9. En un paquete de 9 bits de datos útiles, se añade una redundacia de acuerdo a código polinómico, cuyo polinomio generador es (D4+D+1) (D+1). Indicar cuál de las siguientes respuestas es correcta

a) Si el número de errores es 2, el código siempre los puede corregir.
b) Si el número de errores es impar, la probabilidad de detección es 31/32
c) No todas las situaciones con 2 errores son detectables
d) Ninguna de las anteriores

CORRECTA: D.

a) El código es detector, no corrector
b) Todas las situaciones con un número impar de errores se detectan, ya que se hace uso del factor D+1
c) Se usan 14 bits (9+5). El polinomio generador no es divisor de ningún polinomio de la forma D^j+1, siendo $j<15$, ya que D4+D+1 es primitivo

10. La fuente de un sistema de transmisión de datos tiene un alfabeto de 10 símbolos {0, 1, ..., 9} Cuando el elemento enviado pertenece al conjunto {1, 2, ..., 9} se recibe correctamente, mientras que si el elemento enviado es un 0 se recibe uno del conjunto {1, 2, ..., 9} con probabilidad directamente proporcional al número (por ejemplo, si se envía un 0, la probabilidad de recibir un 5 es 5 veces la probabilidad de recibir un 1).Calcule la capacidad del canal discreto.

a) 3,17 bits/símbolo
b) 3,35 bits/símbolo
c) 3,28 bits/símbolo
d) Ninguna de las anteriores

Correcta: A $\log_2 9$

Dado que la salida tiene un alfabeto de 9 elementos el valor máximo de H(D) es $\log_2 9$. Se puede ver que esa situación es perfectamente compatible con el mínimo de H(D/F), que es 0 cuando p(0)=0.

Por lo tanto máx (H(D)-H(D/F)) = $\log_2 9$

11. Sabiendo que la información mutua entre dos variables aleatorias A y B I(A;B)>0, es falso que

a) H(B/A) < H(B)
b) H(A,B)<H(A) + H(B)
c) H(A/B)>H(A) –H(B)
d) Alguna de las anteriores es falsa

Correcta: b

H(B/A) <H(B). CIERTO

H(A,B)<=H(A)+H(B). Se cumple la igualdad si son independientes, de forma que en este caso sería CIERTO

I(A;B)=H(A) – H(A/B) >0
I(A;B)=H(B) – H(B/A) >0

De ambas ecuaciones
H(A) – H(A/B) = H(B) – H(B/A)
H(A/B)= H(A) – H(B) + H(B/A)
Dado que H(B/A) ≥0
H(A/B)≥ H(A) – H(B), es decir c) es CIERTA

Así pues, la única respuesta falsa es d

$H(A|B) \geq H(A) - H(B) \rightarrow$ CIERTO

12. Un cifrador en flujo consta un LFSR de 4 celdas. Indique la respuesta correcta si el periodo es 13 cuando el estado inicial es D^3+D^2+D+1

a) El polinomio de realimentación es primitivo
b) El polinomio de realimentación puede ser irreducible
c) El cifrador trabaja en modo autosincronizante
d) Ninguna de las anteriores

Se puede ver fácilmente que los únicos polinomios irreducibles de grado 4 son:

D^4+D+1
D^4+D^3+1
$D^4+D^3+D^2+D+1$

Los dos primeros son primitivos, de forma que el periodo sería $15 = 2^4-1$

El otro es el polinomio completo, y el periodo sería 5

Por lo tanto

a) Falsa. El periodo sería 15
b) Falsa. El periodo puede ser 5 0 15, dependiendo del polinomio
c) Cuando se trabaja en modo autosincronizante la secuencia de salida es no periódica

Por lo tanto, la respuesta correcta es d)

13. Una fuente binaria tiene las siguientes propiedades: P(B)=1/3, P(B/B)=0,2. Calcule la eficiencia de una codificación de Huffman extendido de orden 1 (agrupaciones de 2 símbolos).

a) E< 0,77
b) 0,77<=E< 0,85
c) 0,85<=E<0,93
d) E>=0,93

La entropía es 0,88

$$p(B) = p(B/A)\,p(A) + p(B/B)\,p(B) \qquad p(A) + p(B) = 1$$

$$p(A) = 2/3 \qquad p(A/B) = 0'8 \qquad p(B/A) = 0'4 \qquad p(A/A) = 0'6$$

$$H(X/A) = p(A/A)\log_2 \frac{1}{p(A/A)} + p(B/A)\log_2 \frac{1}{p(B/A)} = 0'971$$

$$H(X/B) = p(A/B)\log_2 \frac{1}{p(A/B)} + p(B/B)\log_2 \frac{1}{p(B/B)} = 0'722$$

$$H = H(X/A)\,p(A) + H(X/B)\,p(B) = 0'888$$

Codif. extendido

0 → $p(AA) = p(A)\cdot p(A/A) = \frac{2}{3}\cdot 0'6 = 0'4$ —— $0'4 \to 0$

11 → $p(AB) = p(A)\cdot p(B/A) = \frac{2}{3}\cdot 0'4 = 0'2\hat{6}$ —— $0'6 \to 1$ (10 / 11)

100 → $p(BA) = p(B)\,p(A/B) = \frac{1}{3}\cdot 0'8 = 0'2\hat{6}$ (100) $0'33$

101 → $p(BB) = p(B)\,p(B/B) = \frac{1}{3}\cdot 0'2 = 0'0\hat{6}$ (101)

$\bar{L} = 0'4\cdot 1 + 0'2\hat{6}\cdot 2 + 0'2\hat{6}\cdot 3 + 0'0\hat{6}\cdot 3 = 1'9\hat{3}$ per parelle simbols $\Rightarrow$ $E = \frac{0'888}{1'93/2} = 0'918$

14. Indique cuál de las siguientes afirmaciones es FALSA

a) $27^{30} \bmod 31 = 1$

b) Siendo $135529 = 433 * 313$, se verifica que $42059^{134783} \bmod 135529 = 2710$

c) El número de elementos que tienen inversa respecto a la operación producto en Z_{77} es 60

d) Alguna de las anteriores es falsa

a) Teorema Fermat $a^{p-1} \bmod p = 1 \quad (n=p)$

$n = p = 31 \quad \varphi(31) = 30$

$a^{\varphi(n)} \bmod n = 1 \;,\; mcd(a,n) = 1$

$27^{30} \bmod 31 = 1 \;,\; mcd(27,31) = 1$

b) $n = 135529 = 433 \cdot 313$

$\varphi(n) = 432 \cdot 312 = 134784$

$a^{\varphi(n)-1} \bmod n = a^{-1}$

a^{-1} inverso de a en Z_n

Se verifica la relación si

$a \cdot a^{-1} = 1 + kn$

$42059 \cdot 2710 = 1 + 841 \cdot 135529$

c) $n = 77 = 7 \cdot 11$

$\varphi(n) = 6 \cdot 10 = 60 \Rightarrow$ Cardinal del conjunto reducido de residuos

d) FALSO

y poner estado inicial

15. Sea un cifrador en flujo compuesto por dos LFSR cuyas salidas se unen en una puerta XOR para entregar la secuencia cifrante S. Los polinomios de conexiones asociados son: $C_1(D) = D^5 + D^2 + 1$ (primitivo); $C_2(D) = D5 + D4 + D3 + D2 + D + 1$. El periodo de la secuencia S vale:

   a) 31
   b) 186
   c) 6
   d) Ninguna de las anteriores

y $S(0) = 1$

$L_1 = 2^m - 1 = 2^5 - 1 = 31$

$L_2 = m + 1 = 6$

$L = mcm(L_1, L_2) = mcm(31, 6) = 31 \cdot 6 = 186$

16. Sea una fuente discreta sin memoria que emite cuatro símbolos con probabilidades P(A)=P(B)=1/3; P(C)=2/9; P(D)=1/9. La eficiencia de una codificación de Huffman ternaria vale aproximadamente:

a) 1

b) 0.7823

c) 0.8948

d) Ninguna de las anteriores

(0) A $1/3$ — 0

(1) B $1/3$ — 1

(20) C $2/9$ — 20 — 2

(21) D $1/9$ — 21

(dummy) 0

$$\bar{l} = \frac{2}{3}\cdot 1 + \frac{1}{3}\cdot 2 = \frac{4}{3}$$

$$H(F) = \frac{1}{3}\log_3 3 + \frac{1}{3}\log_3 3 + \frac{1}{9}\log_3 9 + \frac{2}{9}\log_3\left(\frac{9}{2}\right) =$$

$$= 1'193$$

$$E = \frac{H(F)}{\bar{l}} = \frac{4}{3}\,1'193 = 0'8948$$

17. Sabiendo que $N = 9797$ tiene divisores cercanos a su media geométrica, calcule $X = 7^{96005} \bmod 9797$

a) 3243

b) 1816

c) 7010

d) Ninguna de las anteriores

$N = 9797 = 97 \cdot 101$

$\phi(N) = 96 \cdot 100 = 9600$

$X = \left(7^{10 \cdot 9600 + 5}\right) \bmod 9797 = 7^5 \bmod 9797 = 7010$

18. Sea un código de Hamming caracterizado por $g(D) = (D+1)(D^3+D+1)$. Puede afirmarse que:

a) El código tiene una capacidad correctora de 3 borrones

b) La eficiencia del código es del 73.3 %.

c) La ráfaga de error $e(D) = D^{11} + D^4$ es detectable

d) Ninguna de las anteriores

a] Hamming $\Rightarrow d_{min} = 3 \Rightarrow p = 2 \neq 3 \Rightarrow$ FALSO

b] $r = 4 \Rightarrow$ código $(15, 11)$

EFICIENCIA $R = \frac{k}{n} = \frac{11}{15} = 0'7\hat{3}$ ✓

c] $e(D) = D^4 \underbrace{(D^7+1)}_{e'(D)}$

$e'(D) \bmod g(D) = 0$ (POR EL POLINOMIO PRIMITIVO DE GRADO 3)

$\Rightarrow$ NO SE DETECTA

19. Sean F1 = {1, 2, 3} y F2 = {2, 4, 6, 8} dos fuentes equiprobables independientes. Sea una fuente (F) cuya salida es el mínimo común múltiplo de la salida de las fuentes anteriores F = mcm(F1, F2). La entropía (en bits) de F condicionada al valor 6 de F2 H(F—F2=6) vale:

(a) 0 ↳ $H(F \setminus F_2 = 6)$

b) 0.9

c) 1

d) Ninguna de las anteriores

Véase Problema 3 Test 23/01/06

20. Un código ISBN-10 es un código detector de errores no binario (trabaja sobre Z_{11}), e introduce un digito de redundancia a los 9 de información. Suponga que un ISBN introducido correctamente se transmite a través de un canal sin memoria donde la probabilidad de recibir incorrectamente un dígito es $p = 10^{-4}$ y posteriormente se almacena en el receptor. Suponiendo que todo ISBN-10 erróneo detectado se retransmite correctamente, ¿Cuánto vale aproximadamente la probabilidad de que un ISBN-10 incorrecto se almacene en el receptor?

a) $4{,}5 * 10^{-7}$
b) $4{,}1 * 10^{-8}$
c) 10^{-8}
d) Ninguna de las anteriores

PROB NO DETECCIÓN

DEBEN PRODUCIRSE AL MENOS 2 ERRORES Y ADEMÁS EL DIGITO DE PARIDAD DEBE COINCIDIR

$$Pr(\text{2 errores}) \simeq \binom{10}{2} p^2 = 4'5 \cdot 10^{-7}$$

$$\text{PROB}\left(\begin{array}{c}\text{coincidencia}\\ \text{digito paridad}\end{array}\right) = \frac{1}{11}$$

al trabajar en Z_{11}

$$Pr(\text{NO DETECCION}) = Pr(\text{2 errores}) \cdot Pr\left(\text{coincidencia}\right) =$$

$$= \frac{1}{11} \cdot 4'5 \cdot 10^{-7} \simeq 4'1 \cdot 10^{-8}$$